

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

v.

Case No. 19-CR-02

ALEXANDER P. BEBRIS,

Defendant.

**NON-PARTY FACEBOOK, INC.'S RESPONSE TO DEFENDANT'S
SUPPLEMENTAL BRIEF REGARDING HIS MOTION TO SUPPRESS
AND FACEBOOK'S MOTION TO QUASH
DEFENDANT'S RULE 17(a) SUBPOENA**

I. INTRODUCTION

Defendant Alexander P. Bebris ("Defendant") wants an employee from non-party Facebook, Inc. ("Facebook") to provide live testimony, in person or via videoconference, in connection with a motion to suppress. Defendant claims that his Fourth Amendment rights were violated when Facebook found child exploitation materials¹ in his account and submitted a report to NCMEC on the theory that Facebook (a private company) and NCMEC (a non-governmental organization) are state actors. This Court should grant Facebook's Motion to Quash. Defendant's theories are unfounded and the testimony he seeks is cumulative and irrelevant.

Facebook has addressed Defendant's theories in two sworn declarations that are sufficient, as multiple courts have recognized. *See* Fed. R. Crim. P. 17. The Seventh Circuit applies a

¹ Federal law refers to "child pornography." A more appropriate term, however, for images and materials that exploit children is child sexual abuse material ("CSAM") or child exploitation material because the term child pornography suggests that victims might have the capacity to consent to the images, which they obviously do not and cannot. In this brief, Facebook uses "child pornography" only when referring expressly to what federal law says.

case-specific test to determine whether a private party becomes a state actor, and Facebook's declarations establish the facts necessary to decide Defendant's motion: Facebook has an independent business reason to rid its platform of child exploitation materials; Facebook licensed the PhotoDNA software from only another private entity (Microsoft); Facebook did not "coordinate" with NCMEC or the Government about this matter or Defendant; and the Government did not acquiesce in Facebook's search of Defendant's Facebook messages, ask Facebook to search Defendant's messages, or offer Facebook a reward for doing so.

Facebook's declarations also demonstrate that NCMEC's viewing of the images did not exceed the scope of Facebook's private search because a person at Facebook viewed the images immediately before reporting them to NCMEC. These facts are dispositive of the issues raised by Defendant, rendering live testimony duplicative or irrelevant and making compliance with Defendant's subpoena unreasonable and oppressive. *See* Fed. R. Crim. P. 17(c).

Courts regularly rely on declarations like this to adjudicate motions under similar circumstances, and this Court should do the same, despite Defendant's incorrect assertion that the Compulsory Process Clause of the Sixth Amendment gives Defendant the right to compel live, pre-trial testimony from third-party witnesses. To the contrary, the Sixth Amendment "does not guarantee criminal defendants the right to compel the attendance of any and all witnesses." *United States v. Valenzuela-Bernal*, 458 U.S. 858, 867 n.7 (1982). Instead, any right that Defendant has to compel live testimony from Facebook is coextensive with Federal Rule of Criminal Procedure 17. *Id.*; *United States v. Echeles*, 222 F.2d 144, 152 (7th Cir. 1955). Under the Rule 17 analysis, requiring Facebook to prepare and provide a live witness would be unreasonable and oppressive. Defendant's subpoena should therefore be quashed.

II. BACKGROUND

A. Defendant Served Facebook with a Rule 17(a) Subpoena Related to His Motion to Suppress and Facebook Moved to Quash.

Defendant served Facebook with a subpoena under Federal Rule of Criminal Procedure 17(a), seeking live testimony from an employee at a hearing on his motion to suppress. Defendant's motion seeks to suppress child exploitation images that Facebook independently discovered and, immediately after a person viewed them, reported to NCMEC as required by federal law. Declaration of Ryan Mrazik in Support of Facebook's Response to Defendant's Supplemental Brief at Ex. A (attaching the Supplemental Declaration of Michael Francis Xavier Gillin, II, a Facebook employee ("Supp. Decl.")).

Defendant argues Facebook is a "state actor" that violated his Fourth Amendment rights by "searching his private Facebook messages without obtaining a warrant." *See United States v. Bebris*, No. 19-cr-02 (E.D. Wis.), ECF No. 16. He also argues NCMEC is a state actor that exceeded the scope of Facebook's private search, relying on *United States v. Ackerman*, 831 F.3d 1292, 1299 (10th Cir. 2016), which held that a defendant's Fourth Amendment rights were violated when a NCMEC analyst opened an e-mail and attachment that no private party had viewed. *Bebris*, ECF No. 30 at 11; *Ackerman*, 831 F.3d at 1305-06. There, NCMEC's opening "exceeded rather than repeated AOL's private search." *Id.* at 1306. *But see Bebris*, ECF No. 32 (Government's response to motion to suppress) (citing *United States v. Reddick*, 900 F.3d 636, 639 (5th Cir. 2018), *cert. denied*, 139 S. Ct. 1617 (2019)).

Before the hearing, Facebook provided a sworn declaration with facts addressing Defendant's Fourth Amendment theories and also moved to quash the subpoena, arguing that live testimony would be duplicative of the declaration, unreasonable, and oppressive under Federal Rule of Criminal Procedure 17.

B. This Court Held an Evidentiary Hearing.

After Facebook moved to quash the subpoena, this Court held an evidentiary hearing on Defendant's motion to suppress on December 3, 2019. At the hearing, John Shehan, Vice President of the Exploited Child Division at NCMEC, testified via videoconference.² He testified that NCMEC stores the images and hashes it receives from every Electronic Service Provider ("ESP") in NCMEC's industry hash-sharing platform. Specifically, NCMEC uses PhotoDNA to create a digital signature, a "hash," for every image that ESPs report using the CyberTipline. Tr. 21:1-3. NCMEC stores in a database the "signatures" for "every single file from every report [it has] ever received" from an ESP as potential contraband. Tr. 17:7-9; 20:1-8; 21:10-12. Facebook has access to NCMEC's industry and NGO hash databases, and Mr. Shehan is aware that some companies maintain private databases of hash values. Tr. 22:16-17, 23:2-3; 73:23-25.

Mr. Shehan also testified that a NCMEC staff member cannot view an image unless the ESP affirms that an employee has viewed the image. When a CyberTipline Report comes in, a NCMEC staff member is unable to view the image(s) unless the ESP has answered "yes" to whether the "Reporting ESP view[ed] the entire contents of the uploaded file[.]" Tr. 31:9-25. Facebook answered "yes" in both Reports associated with this case. Hr'g. Exs. A, B.

Mr. Shehan discussed the training that NCMEC gives Facebook and other ESPs about the technical specifications and operation of the CyberTipline. Critically, he confirmed that NCMEC does not train Facebook on PhotoDNA or on finding or identifying child pornography. Tr. 25:25-26:3. Mr. Shehan otherwise explained that NCMEC provides training to Facebook and other ESPs about what the fields in the CyberTipline report are, how to use the automatic reporting process, and how the ESP reports appear to NCMEC upon submission of a report. Tr. 25:1-5. He testified

² Defendant had also subpoenaed Microsoft, but Microsoft stipulated to testimony and this Court accepted the stipulation. Tr. 9:9-10.

further that NCMEC will also update Facebook if NCMEC changes the reporting interface for the CyberTipline Reports. Tr. 25:11-17.

After this testimony, Defendant argued that Facebook needed to provide a witness to testify, among other things, about the relationship between Facebook and NCMEC, the source of the hash that identified Defendant's images, and who from Facebook viewed Defendant's images and when. Counsel for Facebook responded that Facebook's declaration was sufficient to resolve the material issues, but would be willing to provide a supplemental declaration on any additional relevant issues because requiring a Facebook employee to provide live testimony would "disrupt[]" the employee's job responsibilities. Tr. 83:15-19; Fed. R. Crim. P. 17(c).

The Court granted Defendant's request to provide supplemental briefing on the need for live testimony from Facebook. Tr. 86:2-20.

C. Defendant Asks Facebook 105 Additional Questions and Submits a Post-hearing Brief.

After the hearing, Defendant submitted 105 questions to Facebook. He then filed a supplemental brief arguing that Facebook must provide live testimony for four reasons.

1. First, he contends that the current declaration from Facebook is insufficient because "knowledge of when and how Facebook determined the images may contain contraband is crucial for this Court to determine whether Bebris's constitutional rights were violated." Def. Supp. Br. 15.
2. Second, he argues that Facebook's declaration is "unreliable" because the declaration stated that "Facebook does not receive training from NCMEC regarding the use or operation of the PhotoDNA software or its processes for reporting to the CyberTipline" but Mr. Shehan testified that NCMEC provides Facebook training on how NCMEC interprets CyberTipline Reports and any changes to the CyberTipline interface. He also argues that Facebook's declaration is inconsistent with statements on Facebook's website that Facebook reports child exploitation content to NCMEC. Def. Supp. Br. at 17.
3. Third, Defendant argues that it is not unreasonable or oppressive for Facebook to provide a live witness in lieu of a declaration because the "requested testimony" is relevant. Def. Supp. Br. 14.

4. Fourth, Defendant argues that the Compulsory Process Clause of the Sixth Amendment compels Facebook, a third party, to provide a live witness at this evidentiary pre-trial hearing.

Facebook, meanwhile, has submitted a supplemental declaration addressing the one issue Defendant actually argues is relevant: that a person at Facebook viewed the images right before submitting the CyberTipline Report. Supp. Decl. ¶¶ 6, 7. The supplemental declaration also clarifies Facebook’s statement that “Facebook does not receive training from NCMEC regarding the use or operation of the PhotoDNA software or its processes for reporting to the CyberTipline.” Indeed, “Facebook does not receive training from NCMEC regarding the use or operation of the PhotoDNA software.” Nor does Facebook “receive training from NCMEC on Facebook’s own internal processes, including Facebook’s use of PhotoDNA or Facebook’s process of determining the content of its CyberTipline reports.” Supp. Decl. ¶ 5; *see supra* (citing Tr. 25:25-26:3). In sum, Facebook’s declarations provide that:

- Facebook has an independent business purpose in keeping its platform safe and free from harmful content and conduct, including content and conduct that sexually exploits children. As Facebook’s Community Standards explain, “We do not allow content that sexually exploits or endangers children. When we become aware of apparent child exploitation, we report it to the National Center for Missing and Exploited Children (NCMEC), in compliance with applicable law.” Supp. Decl. ¶ 3.
- Facebook has no evidence that the Government or NCMEC knew of or acquiesced in Facebook’s search of Defendant’s images. Facebook licensed the PhotoDNA software directly from Microsoft, another private entity, and uses that software to identify child exploitation content as well as other types of violations of its Terms of Service or Community Standards. Facebook does not receive training from NCMEC or the Government about how to use the software. Supp. Decl. ¶ 5.
- Neither the Government nor NCMEC asked Facebook to search Defendant’s Facebook uploads. Facebook has no records of receiving legal process from the Government for the account holders associated with this matter’s CyberTipline Reports or of communicating with the Government about this matter (except regarding Defendant’s instant subpoena). And other than the initial submission of the CyberTipline Reports, Facebook’s declarant is not aware of communications with NCMEC leading up to submission of the reports (let alone of “coordinating” with NCMEC). Supp. Decl. ¶¶ 4, 8.

- Facebook did not receive a reward from the Government or NCMEC for searching Defendant's messages. Supp. Decl. ¶¶ 4, 8.
- A person at Facebook viewed the images in question immediately before that employee reported the images to NCMEC. Supp. Decl. ¶¶ 6, 7. The CyberTipline reports ask: "Did reporting ESP view the entire contents of the uploaded files?" and the reports reflect the answer "Yes." Supp. Decl. ¶¶ 5-6.

III. ARGUMENT

A. Facebook's Declaration, Which It Supplemented, Is Sufficient for the Court to Decide the Issues Relevant to Defendant's Motion to Suppress.

Where (as here) a defendant argues that a private party violated his Fourth Amendment rights, the defendant bears the burden of proving the private entity was functioning as a state actor during the conduct at issue. The Seventh Circuit applies a case-specific four-factor, totality-of-the-circumstances analysis. *See United States v. Gingles*, 467 F.3d 1071, 1074 (7th Cir. 2006); *United States v. Shahid*, 117 F.3d 322, 325 (7th Cir. 1997). Two "critical factors" are (1) "whether the government knew of and acquiesced in the intrusive conduct" and (2) "whether the private party's purpose in conducting the search was to assist law enforcement agents or to further its own ends." *Shahid*, 117 F.3d at 325 (internal quotations and citation omitted). Other criteria are (3) "whether the private actor acted at the request of the government" and (4) "whether the government offered the private actor a reward." *Gingles*, 467 F.3d at 1074 (internal quotations and citation omitted).

No court has held that an ESP acts as an agent of the government by scanning its platform for illegal and violative content, reporting child pornography to NCMEC, or removing child pornography from its services. *See, e.g., United States v. Stevenson*, 727 F.3d 826, 831 (8th Cir. 2013) (holding that the NCMEC reporting obligation does not make a service provider a state actor and recognizing that a provider's "voluntary efforts to achieve a goal that it shares with law enforcement do not, by themselves, transform the company into a government agent"); *United*

States v. Cameron, 699 F.3d 621, 638 (1st Cir. 2012) (reporting obligation does not make a provider a state actor); *United States v. Richardson*, 607 F.3d 357, 366 (4th Cir. 2010) (same).

Under the private-search doctrine, if a private party (not acting as a government agent) discovers information and later reveals that information to the authorities, “the Fourth Amendment does not prohibit governmental use of the now-nonprivate information.” *United States v. Jacobsen*, 466 U.S. 109, 117 (1984); *Ackerman*, 831 F.3d at 1305-06; *Reddick*, 900 F.3d at 639.

1. Facebook Has Addressed the Relevant Issues.

Facebook’s declarations establish the facts that this Court needs to decide Defendant’s motion to suppress: whether Facebook was a state actor under *Shahid* and *Ginglen* when it searched Defendant’s Facebook messages (it was not) and whether NCMEC’s viewing of the two images exceeded the scope of Facebook’s search (it did not).

First, the declarations give the Court everything it needs to assess the four factors to determine whether Facebook was a state actor:

- **Did the government know of or acquiesce in the intrusive conduct?** There is no evidence that the Government knew of or acquiesced in Facebook’s use of PhotoDNA to search Defendant’s Facebook uploads or view his pictures. *See Shahid*, 117 F.3d at 325; Supp. Decl. ¶¶ 3, 4, 8. NCMEC’s knowledge of Facebook’s searches of messages and uploads, meanwhile, is irrelevant. Even if NCMEC is an agent of the government, Defendant has not shown that NCMEC’s knowledge should be imputed to its principal. And there is no evidence that NCMEC had any knowledge that Facebook was searching Defendant’s accounts in particular.
- **Was Facebook’s purpose in conducting the search to assist law enforcement agents or to further its own ends?** Facebook’s “purpose in conducting the search was to . . . further its own ends.” *See Shahid*, 117 F.3d at 325. Specifically, Facebook has an independent business purpose in keeping its platform safe and free from harmful content and conduct, including content and conduct that sexually exploits children. Supp. Decl. ¶¶ 3, 4. As Facebook’s Community Standards explain, Facebook “do[es] not allow content that sexually exploits or endangers children.” Like many other ESPs, Facebook has a business interest in protection against “reputational threats, like images depicting child pornography.” *See Stevenson*, 727 F.3d at 831. Such images may deter others from using the platform. *See id.*

- **Did Facebook act at the request of the government?** No, the Government never asked Facebook to scan Defendant's uploads and messages for child exploitation content. *See Ginglen*, 467 F.3d at 1074; Supp. Decl. ¶¶ 3, 4, 8. Facebook has no records of receiving legal process from the Government for the account holders associated with this matter's CyberTipline Reports or of communicating with the Government about this matter (except regarding Defendant's instant subpoena). Nor did NCMEC ever ask Facebook to scan Defendant's messages and uploads for child exploitation content. See Tr. 53:4-24 (ESPs approach NCMEC to use CyberTipline); Supp. Decl. ¶¶ 3, 4, 8.
- **Did the government offer Facebook a reward?** No, the Government did not offer Facebook a reward for scanning Defendant's messages. *See Ginglen*, 467 F.3d at 1074; Supp. Decl. ¶¶ 3, 4, 8. Nor did NCMEC. Supp. Decl. ¶¶ 3, 4, 8.

Second, neither NCMEC nor the Government exceeded the scope of Facebook's private search when they viewed the two images in question. *See Jacobsen*, 466 U.S. at 117. As explained in Facebook's declarations, a person viewed the child-exploitive images in their entirety immediately before submitting them using the CyberTipline Report. Supp. Decl. ¶¶ 6, 7.

Relatedly, the federal statute requiring ESPs to report to NCMEC any child exploitation content that they discover, 18 U.S.C. § 2258A, is insufficient to make Facebook a state actor. Courts agree that this reporting obligation does not make an ESP a state actor. *Stevenson*, 727 F.3d at 831 (holding that the NCMEC reporting obligation does not make a service provider a state actor); *Cameron*, 699 F.3d at 638 (reporting obligation does not make a provider a state actor); *Richardson*, 607 F.3d at 366 (same); *see generally Ohio v. Clark*, 135 S. Ct. 2173, 2183 (2015) (Ohio statute's requirement that teacher report suspected abuse directly to the government did not transform conversation between teacher and student into a law-enforcement mission). Indeed, the *Shahid/Ginglen* factors confirm that this court has what it needs to decide—as every court before it has decided—that the reporting statute does not and *cannot* turn Facebook into a state actor:

- This statute does not show that Congress or the Government knew that Facebook was searching actively users' uploads and messages for child exploitation content, let alone that it was screening Defendant's content, as it did here. In fact, the statute specifically disclaims any duty to search for content. 18 U.S.C. § 2258A(f).

- The statute does not show that Facebook was acting with the goal of helping law enforcement when it searched Defendant’s Facebook uploads. As discussed above, Facebook has an independent business purpose for identifying and removing child exploitation content. A provider’s “voluntary efforts to achieve a goal that it shares with law enforcement do not, by themselves, transform the company into a government agent.” *Stevenson*, 727 F.3d at 831.
- It does not show that Congress or the Government asked Facebook to search its users’ uploads and messages for child exploitation content at all, let alone to search Defendant’s content.
- The statute offers no reward for an ESP’s reporting at all, let alone with respect to Defendant.

Finally, because the Seventh Circuit’s state action test is case-specific, it is irrelevant whether there are any general connections between Facebook and the Government and Facebook and NCMEC. But even if this Court were to widen the focus of the inquiry to look at the overall relationship between the Government and Facebook, contrary to the Seventh Circuit’s case-specific test, Facebook remains a regulated, for-profit enterprise. Donation to a non-profit organization that shares a goal with the government does not and cannot turn a private corporation into a state actor, nor does a voluntary practice of publishing alerts of missing children. *See Shahid*, 117 F.3d at 325; *Ginglen*, 467 F.3d at 1074 (only discussion of funding in state-actor test is a reward from the government to the private party); *Stevenson*, 727 F.3d at 831 (“voluntary efforts” toward shared goal); Tr. 41:12-16. If it did, many communications providers and other corporations would become state actors for many different purposes. *See, e.g.*, Verizon, Wireless Emergency Alerts FAQs, <https://www.verizonwireless.com/support/wireless-emergency-alerts-faqs/>.

2. Further Testimony About General Practices, Identifying Specific Employees, or Probing Internal Policies and Procedures is Invasive and Unnecessary.

A criminal defendant is not entitled to limitless information from third parties, as Rule 17 “was not intended to provide a means of discovery for criminal cases,” and cannot be used for a

“fishing expedition” for information potentially helpful to a defendant. *United States v. Nixon*, 418 U.S. 683, 698 (1974) (citing *Bowman Dairy Co. v. United States*, 341 U.S. 214, 220 (1951)). Defendant’s subpoena for additional testimony is such a fishing expedition, as the testimony of a Facebook employee would merely duplicate the declarations already provided in violation of Rule 17. *See United States v. Romano*, 482 F. 2d 1183, 1195 (5th Cir. 1973) (it is an abuse of Rule 17 to subpoena a witness whose testimony “would be cumulative only”); *see also Stern v. U.S. Dist. Court for Dist. of Mass.*, 214 F.3d 4, 17 (1st Cir. 2000).

When adjudicating motions to suppress child exploitation content based on theories like Defendant’s, Courts regularly rely on declarations from providers such as Facebook as enough to establish the facts needed to adjudicate the motions. *See, e.g., United States v. Viramontes*, No. 3:16-cr-00508-EMC (N.D. Cal. Mar. 13, 2018) (relying on declaration from Dropbox to adjudicate motion to suppress evidence of various child-pornography-related counts); *United States v. Miller*, No. 16-47-DLB-CJS, 2017 WL 2705962, at *1-2 (E.D. Ky. June 23, 2017) (relying on a declaration and describing Google’s process for the review and reporting of apparent CSAM); *United States v. Lien*, No. 3:16-cr-00393-RS (N.D. Cal. May 10, 2017) (same); *United States v. Wilson*, No. 3:15-CR-02838-GPC, 2017 WL 2733879, at *1-2 (S.D. Cal. June 26, 2017) (same).

All of the information that Defendant argues is missing from Facebook’s declaration is either included or irrelevant.

Defendant argues that Facebook’s declaration is insufficient because it does not name the Facebook employee who viewed the images, Def. Supp. Br. at 14-15, but the Court does not need to know which Facebook employee viewed the images to determine whether a Facebook employee viewed the images. *United States v. Keith*, the case defendant relies upon, is inapposite. 980 F.

Supp. 2d 33 (D. Mass. 2013). In that case, “no AOL employee opened or viewed the file before it was forwarded to NCMEC.” *Id.* at 37.

Any remaining questions about Facebook, *see* Def. Supp. Br. at 14-15, are either sufficiently answered in Facebook’s declarations and/or irrelevant.

- How Facebook uses the hash values from NCMEC’s so-called “Hash Value Database” once it retrieves them
 - Facebook’s general practices are irrelevant to Defendant’s particular case. Also, Facebook generally uses PhotoDNA software to match uploaded images with hash values. Supp. Decl. ¶ 4; *see also* Tr. 65:6-13.
- Whether an image was detected through PhotoDNA or a member of the public
 - Facebook explained in its declaration that it became aware of Defendant’s images through PhotoDNA. Supp. Decl. ¶¶ 5, 6.
- “[H]ow [Facebook is] detecting and becoming aware of the incidents”
 - Facebook explained in its declaration that it became aware of Defendant’s images through PhotoDNA. Supp. Decl. ¶¶ 5, 6.
- How Facebook uses the field on the CyberTipline Report stating that someone viewed the images
 - Facebook has sufficiently explained that a “yes” response to whether the reporting ESP viewed the entire contents of uploaded files indicates that the images were viewed immediately prior to submitting the CyberTipline Report to NCMEC. Supp. Decl. ¶¶ 6, 7.
- Whether Facebook is developing or implementing AI technology to search for child exploitation content on its servers and site
 - Facebook identified the two images at issue here using PhotoDNA, not artificial intelligence. Supp. Decl. ¶ 6.
- Whether Mr. Barry viewed the uploaded file
 - As explained above, the name of the Facebook employee who viewed the images is not necessary to determine whether a Facebook employee viewed the images.
- When “someone within [Facebook] viewed [the two images]”
 - Facebook’s supplemental declaration clarifies that a person viewed the

images immediately before submission to NCMEC. Supp. Decl. ¶¶ 6, 7.

- Whether the two files were in the so-called NCMEC “Hash Value Database” or another hash set that private companies are sharing
 - Defendant makes no argument for this information’s relevance. In any event, the source of the hash is irrelevant. Whether the hash came from NCMEC’s Industry Database or a private company’s database, the original source of the hash value is a private party. *See* Tr. 21:10-12. As a result, a private party identified the hashes that matched with Defendant’s uploaded images. As a result, NCMEC’s and the government’s “search” did not exceed the private parties’.
- Whether Facebook is working to help NCMEC develop new software to help prioritize reports
 - Facebook reported Defendant’s two images through the legally mandated CyberTipline Reporting process. Supp. Decl. ¶¶ 3, 6. How those images are technically processed after submission is irrelevant to the state actor analysis. In addition, Facebook’s other general endeavors to provide technical support or resources in the fight against child exploitation are irrelevant.
- How Facebook’s automated reporting system works
 - Facebook has already explained how it reported Defendant’s images to NCMEC as required by law. Supp. Decl. ¶¶ 3, 5, 6, 7.

Testimony from Facebook about general practices, policies, and procedures is irrelevant and unnecessary. As mentioned above, the state-actor test is case-specific: the defendant must demonstrate that the private entity was acting on behalf of the government when it engaged in the conduct at issue. For example, in the *Stevenson* case, the court observed that “the government never asked AOL to scan Stevenson’s e-mail.” 727 F.3d at 831. In *Ginglen*, the Seventh Circuit evaluated whether the private individuals “were acting as private individuals *when they entered the home.*” 467 F.3d at 1073 (emphasis added). The general relationship between the government and the private actor, especially in unrelated engagements, is irrelevant.

Defendant’s assertion that Facebook’s declaration is “unreliable” is misplaced. Facebook’s declaration stated that it did not “receive training from NCMEC regarding the use or

operation of the PhotoDNA software or its processes for reporting to the CyberTipline.” Facebook’s supplemental declaration states that, although it receives training from NCMEC about how *NCMEC* uses the fields in the CyberTipline Reports, Facebook does not “receive training from NCMEC *regarding the use or operation of the PhotoDNA software.*” Nor does Facebook receive training from NCMEC about Facebook’s internal processes for reporting to the CyberTipline. Facebook’s processes for creating CyberTipline Reports are determined internally. Supp. Decl. ¶ 5.

Additionally, Facebook’s website is consistent with its declarations. Facebook’s website says that Facebook’s “Community Standards ban child exploitation.” Facebook, “New Technology to Fight Child Exploitation” (Oct. 24, 2018), *available at* <https://about.fb.com/news/2018/10/fighting-child-exploitation/>). The website further states that, as one prong of Facebook’s strategy to “keep[] children safe on Facebook,” Facebook “report[s]” child exploitation images to NCMEC. *Id.* Facebook also “remove[s] accounts that promote this type of content,” requires children to be at least 13 years old to sign up, and limits the people with whom teenagers can interact on Facebook. *Id.*

Defendant concedes that Rule 17 does not require a live witness to give duplicative testimony. *See* Def. Supp. Br. at 14. Yet the information Defendant seeks to elicit via live testimony is all duplicative or irrelevant. The Court should therefore quash Defendant’s subpoena.

B. The Compulsory Process Clause Does Not Require Live Testimony at All.

Finally, Defendant incorrectly claims that although Rule 17 does not require live witnesses to give duplicative testimony, Facebook’s testimony is required under the compulsory process clause of the Sixth Amendment to the United States Constitution. But no court has ever held that the Sixth Amendment creates a right to compel non-parties to provide duplicative testimony in pretrial proceedings.

The Sixth Amendment to the United States Constitution guarantees that “[i]n all criminal prosecutions the accused shall enjoy the right . . . to have compulsory process for obtaining witnesses in his favor.” U.S. Const. amend. VI. But this right is not unlimited—the Supreme Court has never held that this clause creates a right to pretrial testimony from a third party. After all, “[t]here is no general constitutional right to discovery in a criminal case.” *Weatherford v. Bursey*, 429 U.S. 545, 559 (1977). The Supreme Court’s compulsory-process cases “establish . . . that criminal defendants have the right to the government’s assistance in compelling the attendance of favorable witnesses at trial.” *Pennsylvania v. Ritchie*, 480 U.S. 39, 56 (1986) (plurality opinion) (emphasis added). But the United States Supreme Court has “never squarely held that the Compulsory Process Clause guarantees the right to discover the identity of witnesses, or to require [even] the *government* to produce exculpatory evidence” during pretrial discovery. *Id.* at 56 (emphasis added); *see also id.* at 53-54 & n.6 (holding that the Confrontation Clause “does not include the power to require the pretrial disclosure of any and all information that might be useful in contradicting unfavorable testimony”).

“That the Sixth Amendment does not guarantee criminal defendants the right to compel the attendance of any and all witnesses is reflected in the Federal Rules of Criminal Procedure,” including Rule 17. *Valenzuela-Bernal*, 458 U.S. at 867 n.7; *United States v. Echeles*, 222 F.2d 144, 152 (7th Cir. 1955). “A defendant’s right to present relevant evidence is not unlimited, but rather is subject to reasonable restrictions.” *United States v. Scheffer*, 523 U.S. 303, 308 (1998). Indeed, Rule 17(c) allows a court to quash or modify a subpoena if “compliance would be unreasonable or oppressive,” such as where a subpoena seeks cumulative or duplicative evidence. *See supra* Part III.A.2; *Romano*, 482 F.2d at 1195.

To prove a violation of the Compulsory Process Clause, a defendant must “make a

plausible showing that the testimony . . . would have been material and favorable to his defense, in ways not merely cumulative” of other testimony. *Valenzuela-Bernal*, 458 U.S. at 873. Here, quashing the subpoena under Federal Rule of Criminal Procedure 17(c) would not violate Defendant’s Sixth Amendment rights.³ *Id.* at 867 n.7; *Echeles*, 222 F.2d at 152. Defendant has no Sixth Amendment right to compel a non-party, Facebook, to produce a live witness during a pretrial proceeding. *See Bursey*, 429 U.S. at 559; *Ritchie*, 480 U.S. at 56 (plurality op.). Moreover, as discussed above, the testimony of Facebook’s live witness would be “cumulative” of its declarations. *See Valenzuela-Bernal*, 458 U.S. at 873.

Defendant relies on a statement from the Supreme Court in *United States v. Nixon* to argue that “[a] defendant’s compulsory right extends to both trial and pretrial proceedings.” But the statement on which Defendant relies simply says that “[e]nforcement of a pretrial subpoena duces tecum” is “committed to the sound discretion of the trial court.” 418 U.S. 683, 702 (1974). This confirms that courts can (as the *Nixon* court did) analyze the validity of a subpoena duces tecum under Rule 17(c)’s standards. *See id.* at 697-702; *Echeles*, 222 F.2d at 152. It does not mean that Defendant has a constitutional right to mandate live witnesses from third parties during pretrial proceedings, particularly where the testimony sought is duplicative and cumulative. Indeed, as Defendant concedes, “federal criminal procedure rules implement the right to compulsory process in federal cases.” *See* Def. Supp. Br. 20.

Finally, Defendant’s conclusory statement that “any testimony to the extent [sic] of the partnership between Facebook and NCMEC will weigh in Bebris’s favor” is unavailing. Def. Supp. Br. at 22. Any testimony about the alleged “partnership” between Facebook and NCMEC will be either duplicative or irrelevant and thus immaterial. *See Valenzuela-Bernal*, 458 U.S. at

³ Defendant concedes that the Confrontation Clause, which provides defendants a right to confront witnesses, does not apply here. *Compare* Tr. 85:23-25, *with* Def. Supp. Br.

873 (“merely cumulative”). Facebook’s alleged “partnership” with NCMEC does not affect whether Facebook was acting as a *government* agent when it discovered Defendant’s images. The state-actor test asks whether the *government* knew of Facebook’s search of *Defendant’s* uploads, whether the *government* asked Facebook to search *Defendant’s* Facebook uploads, whether the *government* offered Facebook a reward for searching *Defendant’s* uploads, and whether Facebook was acting to further its own ends when it searched *Defendant’s* uploads. No one is arguing that NCMEC is the government, and Facebook’s alleged “partnership” with NCMEC does not affect whether NCMEC’s viewing of Defendant’s images exceeded the scope of Facebook’s private search. The fact that a person, acting consistently with Facebook policies and for internal business purposes, identified and viewed the images immediately before submitting them to NCMEC is dispositive of the Fourth Amendment analysis.

IV. CONCLUSION

For these reasons, Facebook respectfully requests that this Court quash Defendant’s Rule 17(a) subpoena.

DATED: January 10, 2020

Respectfully submitted,

By: /s/ Ryan T. Mrazik
Ryan T. Mrazik
PERKINS COIE LLP
1201 3rd Ave - Ste 4900
Seattle, WA 98101
rmrazik@perkinscoie.com
Telephone: 206.359.8000

Attorney for Facebook, Inc.